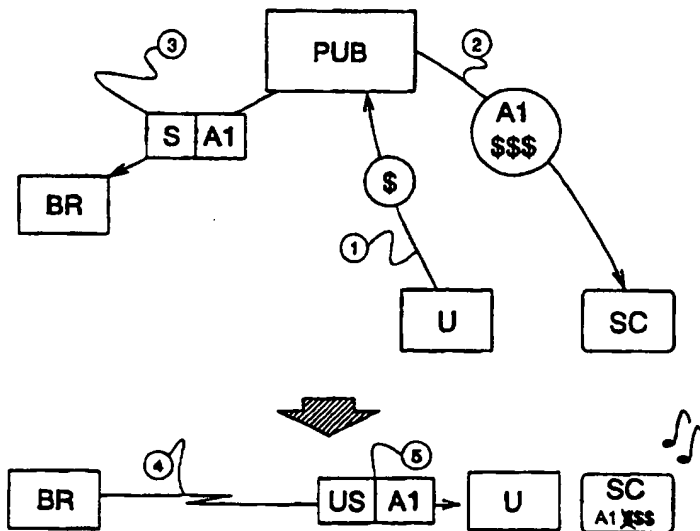


INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04N 7/167		A1	(11) International Publication Number: WO 97/28649
			(43) International Publication Date: 7 August 1997 (07.08.97)
(21) International Application Number: PCT/FI97/00045		(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).	
(22) International Filing Date: 29 January 1997 (29.01.97)			
(30) Priority Data: 960418 30 January 1996 (30.01.96) FI			
(71) Applicant (for all designated States except US): OY NOKIA AB [FI/FI]; Eteläesplanadi 12, FIN-00130 Helsinki (FI).			
(72) Inventor; and		Published With international search report.	
(75) Inventor/Applicant (for US only): SALOMÄKI, Ari [FI/FI]; Auertie 7 C 42, FIN-04400 Järvenpää (FI).			
(74) Agent: BERGGREN OY AB; P.O. Box 16, FIN-00101 Helsinki (FI).			

(54) Title: SCRAMBLING OF DIGITAL MEDIA OBJECTS IN CONNECTION WITH TRANSMISSION AND STORAGE



(57) Abstract

To prevent unauthorized reception, storage, copying and reproduction of digital media objects, it is defined in addition to a scrambled broadcast format a scrambled storage format which is different from the broadcast format. A user's terminal equipment cannot receive, store or reproduce protected objects without a key which is advantageously a bit sequence stored on a portable memory medium and which can be different according to the type of use it gives entitlement to. To prevent the storing and later reproduction as such of data in the broadcast format, a time stamp is included in the broadcast format representing the time of broadcasting. A playback device cannot reproduce a broadcast-format object if the reproduction time differs from the time stamp included in the broadcast format. The reproduction time is advantageously read from a real time clock of a portable memory medium.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	GB	United Kingdom	MW	Malawi
AT	Austria	GE	Georgia	MX	Mexico
AU	Australia	GN	Guinea	NE	Niger
BB	Barbados	GR	Greece	NL	Netherlands
BE	Belgium	HU	Hungary	NO	Norway
BF	Burkina Faso	IE	Ireland	NZ	New Zealand
BG	Bulgaria	IT	Italy	PL	Poland
BJ	Benin	JP	Japan	PT	Portugal
BR	Brazil	KE	Kenya	RO	Romania
BY	Belarus	KG	Kyrgyzstan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic	KR	Republic of Korea	SE	Sweden
CG	Congo	KZ	Kazakhstan	SG	Singapore
CH	Switzerland	LI	Liechtenstein	SI	Slovenia
CI	Côte d'Ivoire	LK	Sri Lanka	SK	Slovakia
CM	Cameroon	LR	Liberia	SN	Senegal
CN	China	LT	Lithuania	SZ	Swaziland
CS	Czechoslovakia	LU	Luxembourg	TD	Chad
CZ	Czech Republic	LV	Latvia	TG	Togo
DE	Germany	MC	Monaco	TJ	Tajikistan
DK	Denmark	MD	Republic of Moldova	TT	Trinidad and Tobago
EE	Estonia	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	UG	Uganda
FI	Finland	MN	Mongolia	US	United States of America
FR	France	MR	Mauritania	UZ	Uzbekistan
GA	Gabon			VN	Viet Nam

Scrambling of digital media objects in connection with transmission and storage

5 The invention relates in general to the protection of digital sound and picture objects against unauthorized reception and copying and in particular to how the protection against unauthorized reception and copying can be implemented in a uniform manner as regards broadcasting, local storage and the selling and distribution of recordings to consumers.

10 Electrical transmission and storage of programs and presentations including images and/or sound has shifted or is shifting from analog to digital technology, the advantages of the latter being lower susceptibility to spurious effects and versatile error correction possibilities. The quality of a digital image and sound will not deteriorate in transmission, reception and storage in the same way as it does when
15 using analog technology. Digital technology is already being widely used in the sales and distribution of audio and data recordings in the form of compact discs, or CDs. Computers apply digital magnetic storing of data in their mass memory units and digital broadcasting systems are in pilot stages. We can assume that in the future both the capacity and the exploitation of data transmission and storage will
20 continue to increase.

Below, all digital sound and image recordings and transmissions handled as one entity will be called simply objects. An object may be a picture, sound effect, piece of music, film, animated program, radio program, multimedia program or other
25 corresponding entity which can be transmitted, stored and reproduced to a user as such and/or together with other corresponding objects. By transmission it is meant especially broadcasting, where a transmitting station electrically distributes objects to a great number of receivers on a regular basis. By storing it is meant that the object or a period extracted from it is rendered into a form from which it can be
30 later decoded to be reproduced to a user several times if required.

Computer programs can also be considered some kind of objects, even though they are not in the same way meant to be broadcast. Multimedia and interactive mass media becoming more popular, the boundary between the computer program as we
35 know it and the radio or TV program, whether it is meant to be entertaining or educational, will become blurred. For instance, the digital audio broadcasting (DAB) system provides for transmitting objects that are broadcast in file format and loaded in the storage media of the receiving equipment to be later interactively

reproduced to a user so that the user will have the opportunity to change the flow of the program.

5 Since digital recordings are easily duplicated, there has arisen a need to encrypt, or scramble, the objects in connection with transmission and storage so that their reception and reproduction without a permission from their copyright owners be as difficult as possible. The purpose of this arrangement is that the producer and/or distributor of an object get a certain remuneration from the receiver and/or user. It is common that a user acquires a decoding device or key with which the object can be
10 descrambled for use. A so-called black box is known from the prior art which descrambles programs sent on TV channels liable to charges. A descrambling device may be controlled by a so-called smart card, for example, which contains the code words needed for descrambling. A similar method, where a scrambled transmission is descrambled using keys stored in a smart card, has been applied in digital data
15 transmission in the GSM mobile telephone system, for example.

Scrambling and descrambling methods and devices according to the prior art are usually characterized in that they are channel specific which means the scrambling is directed to a particular transmission stream always in the same way regardless of
20 what objects the transmission stream contains. The only options are switching the scrambling on and off, if e.g. a pay TV channel wants to send a particular film or program unscrambled so that it can be viewed by a larger audience. Copyrights, however, are always directed to individual objects and, therefore, methods according to the prior art cannot implement a pay system where the producers of objects
25 acquired from different sources could be remunerated in any other way than if the transmitting station pays for the right to broadcast a particular object in its distribution network or coverage area.

Arrangements according to the prior art are also characterized in that a receiver who
30 has at his disposal a descrambling device can without limitation store, duplicate and further distribute a particular object after having descrambled it. To safeguard the rights of parties producing objects and their transmission and distribution services it is essential that users could be obliged to pay a separate recompense for storing and duplicating an object.

35 In conjunction with computer software it is used a fixed key device, or a so-called hardlock, which usually comprises an electric circuit cast in a plastic housing that has to be inserted in the communications port of the computer for the program to be

usable. With this arrangement it is to some extent possible to prevent the duplication of an object because an ordinary user cannot duplicate the hardlock and a duplicated program copy will not function without the hardlock. However, the arrangement is rather inflexible as the hardlock is tied to a particular version of a particular object, and it cannot be applied on a broader basis if the objects vary and change constantly as they do in a broadcast-type transmission.

An object of this invention is to provide a method for scrambling and descrambling electrically transmitted objects, covering the transmission, reception, storing and reproduction of objects. Another object of the invention is to provide a method which attaches to said scrambling a payment system whereby recompenses corresponding to the descrambling rights are directed to parties producing objects and transmission and distribution services for the objects. A further object of the invention is that the method according to it be applicable to known digital transmission and storing arrangements.

The objects of the invention are achieved by defining general, standardized scrambling data formats to be applied in the broadcasting and storage of digital data, using different scrambling data formats for storing and broadcasting. The achievement of the objects of the invention can be further advanced by adding to the user's descrambling device a real time clock, combining a real time code to the digital broadcast format and by combining the payment transactions corresponding to the descrambling rights to the distribution of descrambling keys.

The method according to the invention for protecting digital media objects against unauthorized use, which objects can be electrically distributed to several receivers and stored on a memory medium for later use, wherein a scrambled broadcast format is specified for said media objects, is characterized in that a scrambled storage format is also specified for said media objects for the storing on said memory medium, which scrambled storage format is different from said scrambled broadcast format.

The invention is also directed to terminal equipment for receiving, storing and reproducing digital media objects to a user, said terminal equipment comprising means for descrambling the scrambled broadcast format. The terminal equipment according to the invention is characterized in that it further includes means for storing a received media object in a scrambled storage format which is different from said scrambled broadcast format.

The invention implies that a common international agreement or standard can define different scrambled formats or identification procedures for digital media objects according to whether they are being transmitted or stored. In addition, different
5 formats or identification procedures can be specified for an object according to whether it is the original version (produced by the copyright owner) or a copy produced by someone else. Devices handling digital media objects are manufactured such that they can reproduce a received or stored object only if they have at their disposal the key that authorizes the reproduction of the object in question. Further-
10 more, in an advantageous embodiment of the invention, the devices will not store broadcast-format objects but will first convert them into the storage format. Objects are advantageously handled as constant-size data parts, or frames, so that the difference between the broadcast format and storage format may be as small as a change of one bit or bit combination in the frame header part or other data structure
15 describing the contents of the packet.

The scrambling method according to the invention further comprises a timing arrangement wherein the objects transmitted are time-stamped, ie. provided with data representing the transmission moment. Then, even if an object were stored in the
20 broadcast format, its unauthorized reproduction at a later time can be prevented if the reproducing device first has to compare the stored time data to the real time. If the times are unidentical, reproduction is prohibited. The timing arrangement is based on an electrical memory medium which is advantageously a smart card or such. Below, this portable memory medium will be called a smart card. In the ar-
25 rangement according to a preferred embodiment of the invention the smart card includes a real time clock, which refers to any circuit in general which, when read at an arbitrary moment of time, unequivocally yields the data representing the time of the reading. According to the invention, each object is arranged both for trans-
mission and storage into data parts that can be called frames, packets, cells or data
30 groups and that are formatted according to existing standards and recommendations describing data transmission and/or storage. At least part of the frames and data groups are provided with a time stamp which in the case of broadcasting refers to the time of transmission and in the case of storage to the time of storing.

35 The contents of an object to be transmitted or distributed as an original recording (such as a CD) are scrambled using a known method where descrambling requires a certain cipher key which advantageously is a relatively big binary number. A user may purchase the right to use the object in question so that when he pays a certain

sum of money, the necessary key or keys will be loaded into his smart card. A key may be valid for a fixed or an indefinite period of time. In the case of a transmitted object the user pays a different sum according to whether he uses the object just once (real time use) or stores (copies) it to be used later and possibly several times.

5 'Using' here means broadly viewing, listening to or otherwise exploiting the object. Because of the different prices for the real time use and storage the keys stored in the smart card have to be different for the different purposes of use.

10 The invention is described in more detail with reference to the preferred embodiments presented by way of example and to the attached drawing, in which

- Fig. 1 shows one phase in the application of the method according to the invention,
- 15 Fig. 2 shows as a series of pictures other phases in the application of the method according to the invention,
- Fig. 3 shows an alternative way of applying the method according to the invention, and
- Fig. 4 shows another alternative way of applying the method according to the invention.

20

Like elements in the drawing are depicted by like reference designators.

Since the invention provides for the broadcasting of digital objects, it will be first described the essential features of the digital audio broadcasting (DAB) system used

25 here as an illustrative application. In the DAB system, the information in an audio transmission and in a data transmission in general is transported in constant-size data parts that in the case of an audio transmission are called audio frames and in the case of a data transmission data groups. Each audio frame and data group includes a header part containing records or fields describing its contents, and a

30 payload part that contains the actual data to be transmitted. In addition, the DAB system specifies in the way known to one skilled in the art data structures that are used for transferring both frame-specific and more general control information from the transmitting to the receiving device. The most important forms of such data structures are the fast information groups (FIG) transferred on the so-called fast

35 information channel (FIC) and, in the case of audio frames, the frame-specific program associated data (PAD) fields.

The DAB system specifies the following audio frame specific data and their transmission along with a scrambled audio broadcast:

1a) scrambling of frame with a known or encrypted key

- 5 In the DAB system, scrambling and encrypting mean different things. Scrambling means changing the audio data such that the sound contained in it cannot be reproduced without knowing a certain key. Said key is a number which, when fed as a seed to a certain generator producing pseudo-random numbers, produces a pseudo-random bit sequence corresponding to the key in
- 10 question. A logical XOR (exclusive-OR) operation executed between the bit sequence and the scrambled audio data produces reproducible audio data. This operation opposite to scrambling is called descrambling. The key, which is given to the user, may be clear (known) or encrypted; in the latter case, the encrypted key must first be decrypted. There exist several arrangements to
- 15 implement the encryption of the key and we will return to them later on. This paragraph refers to the fact that the audio frame specific data in the DAB system indicate whether the frame in question is scrambled using a known or an encrypted key.

20 1b) conditional access system used

- The encryption procedure as a wider concept is included in the conditional access system which includes several specifications related to the access rights of services. Known conditional access systems include Eurocrypt and NR-MSK, among others. The conditional access system applied can be indicated
- 25 for each frame.

1c) cryptoalgorithm

- Code for a certain algorithm identifying the calculatory method applied in the key encryption procedure.
- 30

1d) time stamp

- A time stamp referring to the date and/or time of day can be included in the frames so that it corresponds to the time of transmission.

35 1e) authorization data

- Frames can include identification information which identifies the object transmitted and e.g. the party that produced the object and is the holder of the copyright of the object.

1f) encrypted key

1g) initialization modifiers

- 5 Typically, a scrambling key is valid for a few frames only. Furthermore, a so-called initialization, or reset, can be performed between those frames, too, resetting the pseudo-random bit sequence generator used in the descrambling so that possible errors in the long bit sequence be less harmful. The initialization modifiers define how the generator will be initialized.

10

1h) scrambled audio frame to be transmitted

In addition, the DAB system specifies the following data group specific information and its transmission along with a scrambled data transmission:

15

2a) scrambling of frame with a known or encrypted key

Same as 1a.

2b) conditional access system used

20

Same as 1b.

2c) cryptoalgorithm

Same as 1c.

25

2d) time stamp

Same as 1d.

2e) authorization data

Same as 1e.

30

2f) encrypted key

2g) initialization modifiers

Same as 1g.

35

2h) scrambled data group to be transmitted

In addition, the DAB recommendations specify file-specific transmission as regards the following information:

- 5 2i) file name or id number
- 2j) number of data groups (blocks, segments) in the file
- 2k) file size in bytes
- 10 2l) file version number for modified files.

Next, we will have a look at the frame specific data that according to the invention will be attached to audio frames to be stored. The number, order and size of the records presented as well as the bit value and bit combination definitions are given
15 by way of example only and are not intended to limit the invention.

- 3a) audio frame count, 24 bits
20 Stored frames related to a particular object are consecutively numbered. The proposed 24-bit numbering field can be used to identify 2^{24} frames. If each frame corresponds, according to the DAB standard, to a 24-millisecond playback period, the maximum duration of the stored object is about $4\frac{1}{2}$ days. The consecutive numbering of frames is advantageous especially in operations such as fast rewind, fast forward and search.
- 25 3b) original / copy, 1 bit
One so-called flag bit indicates whether the object is an original version or a copy. For example, flag bit value 1 refers to an original and 0 to a copy. A storing (copying) device has to be built such that it sets the frame-specific flag bit to 0.
- 30 3c) storage attributes, 2 bits
With two bits it is possible to indicate what kind of use is allowed for the object in question. The tables below show an advantageous specification of bit combinations.
- 35

table 1: scrambled audio object

bit b1	bit b0	meaning
0	0	original object and copy can be stored unscrambled
0	1	original object and copy can be stored scrambled
1	0	original object can be stored unscrambled but copy cannot be stored
1	1	original object can be stored scrambled but copy cannot be stored

table 2: unscrambled audio object

5

bit b1	bit b0	meaning
0	0 or 1	original object and copy can be stored unscrambled
1	0 or 1	original object can be stored unscrambled but copy cannot be stored

3d) frame scrambled bit, 1 bit

10 One flag bit indicates whether the frame in question is scrambled or not. Inside a scrambled object there may be unscrambled frames, so it is advantageous to have a frame-specific scrambling indication.

3e) frame scrambled with a known or encrypted key, 1 bit

15 Same as 1a. Flag bit value 1 corresponds to a clear key and value 0 to an encrypted key.

3f) conditional access system used, 3 bits

Same as 1b. With three bits it is possible to identify 8 different conditional access systems at the most.

20 3g) cryptoalgorithm, 6 bits

Same as 1c. With six bits it is possible to identify 64 different crypto-algorithms at the most.

3h) storage information, 21 bits

25 This field is divided into two subfields:

* storage medium identifier, 4 bits, e.g. as in the table below (rest of the bit combinations are reserved for future expansion)

b3			b0	medium
0	0	0	0	broadcast
0	0	0	1	tape
0	0	1	0	CD
0	0	1	1	hard disk
0	1	0	0	remote storage, e.g. in local area network

5 * date, 8 + 4 + 5 bits, including the last two digits of the year (0 to 9, both coded with 4 bits), the ordinal number of the month (1 to 12 coded with 4 bits) and the day of the month (1 to 31 coded with 5 bits) and corresponding in the case of local storage to the storage date and in the case of broadcast or network storage the current date.

10

3i) authorization data, 261 bits

Since the total number of bits presented so far is not divisible evenly by 8 and since it is advantageous to begin certain byte specific data from the byte boundary, this field advantageously starts with 5 padding bits which are all ones. They are followed by a 32-byte (256-bit) authorization data field which can contain information depending on the conditional access system used, such as the service provider identification code, program identification code and program classification.

20 3j) encrypted or unencrypted key, 168 bits

This field is divided into three subfields that are as follows:

- * number of remaining frames with a key (8 bits), which indicates for how long the current key will be used for descrambling,
- * current key (80 bits), and
- 25 * next key (80 bits).

The two-key arrangement gives to the receiving or reproducing device time to decrypt the next encrypted key. When the count of remaining frames reaches zero, the new key becomes the current key and the next key becomes the new key. The real length of the key depends on the scrambling system used and on the encryption method of the key, so the 80 bits mentioned here is just the maximum length.

30

3k) initialization modifiers, 40 bits

Same as 1g.

5 3l) standard for the audio frame structure, 8 bits

Since, according to the invention, the storage format is not tied to any particular audio frame structure, it is advantageous to indicate in the stored frame data the standard with which the frame complies. The frame may be e.g. an ISO/IEC 11172-3 Layer II or Layer III frame in accordance with the motion picture experts group (MPEG) standards or a DAB audio frame. When coding the standard identifier with eight bits, ample space is left in reserve for future frame standards.

3m) hash sum for 3a to 3l, 88 bits

15 The fields described above in 3a to 3l are advantageously left unscrambled so that they can be read as quickly as possible in connection with reception and/or playback. However, they have to be somehow protected against unauthorized modification. According to the invention, a so-called hash algorithm is used in a known manner, said algorithm being identified by the 8 first bits in the 3m field and used to calculate a certain 80-bit result on the basis of the bit contents of said fields. By comparing the contents of fields 3a through 3l to the hash sum it is possible to detect whether the contents of the fields have been changed after the hash sum was calculated. Since an unauthorized device does not know the hash algorithm, it cannot change the hash sum to correspond to the modified header field values.

3n) stored scrambled or unscrambled audio frame, variable length

30 In the beginning of the frame there is a 16-bit length subfield indicating the length of the audio frame in bytes. The length of the frame depends on the encoding method, level of compression and possible ancillary data (program associated data, PAD, in the DAB). Inclusion of the length information in the beginning of the frame helps operations such as fast rewind, fast forward and search.

35 Next, we will have a look at the data group specific information attached according to the invention to the data groups stored. From the point of view of the invention it is not essential how the file specific information (2i to 2l) is stored since according to the invention the scrambling and protection arrangements are performed on the

data group level. The number, order and size of the records presented and the bit value and bit combination specifications are presented by way of example only and are not intended to limit the invention.

- 5 4a) data group numbering, 24 bits
 Data groups related to a particular file are consecutively numbered. In this sense, the data groups can be called blocks or segments. The consecutive numbering is advantageous especially in operations such fast rewind, fast forward and search.
- 10 4b) original / copy, 1 bit
 Same as 3b.
- 4c) storage attributes, 2 bits
15 Same as 3c.
- 4d) data group scrambled bit, 1 bit
 Same as 3d.
- 20 4e) data group scrambled with a known or an encrypted key, 1 bit
 Same as 3e.
- 4f) conditional access system used, 3 bits
 Same as 3f.
- 25 4g) cryptoalgorithm, 6 bits
 Same as 3g.
- 4h) storage information, 21 bits
30 Same as 3h.
- 4i) authorization data, 261 bits
 Same as 3i.
- 35 4j) encrypted or unencrypted key, 168 bits
 Same as 3j.

4k) initialization modifiers, 40 bits

Same as 3k.

4l) hash sum for 4a to 4k, 88 bits

5 Same as 3m.

4m) stored scrambled or unscrambled data group, variable length

Same as 3n.

- 10 Let us next consider the real time clock in the smart card as part of the implement-
ation of the arrangement according to the invention. There are good reasons to in-
clude the real time clock in the system because then it becomes possible to dis-
tinguish between the immediate reproduction of a received broadcast object and a
later reproduction of an object stored (illegally) in the broadcast format. As was
15 mentioned earlier, devices that store digital objects should be designed and built
such that they cannot store objects in the broadcast format but in connection with
the storing change certain bits in the storage information field (3h / 4h above) so
that they indicate the storage medium. However, it is possible to build a "pirate"
device that does not change the bits in question but simply stores the object in the
20 broadcast format. But as the pirate device does not know the calculation algorithm
for the hash sum (3m / 4l above) it cannot change the frame or data group time
stamp and calculate a corresponding new hash sum. Since it is required of re-
production devices that they compare the time stamps in the frames or data groups
of broadcast-format objects to their own real time clocks before allowing re-
25 production. a recording made by a pirate device can be reproduced only using a
similar pirate device where the time stamp comparison to the real time clock is
bypassed. It is, however, probable that all legally sold reproduction devices include
said comparison feature, so the arrangement can at least to a large extent prevent the
sales of pirate copies stored in the broadcast format to those users who own a legal
30 device.

Said real time clock is advantageously located in the smart card because then its
unauthorized changing can be prevented in the same known way as the changing of
other information in the smart card. Furthermore, it can be required that when a user
35 presents his smart card to an authorized dealer for new keys to be loaded in it in the
manner described later on, the new keys will not be loaded if the clock in the smart
card has been tampered with. If the time stamps are made, as proposed above, at the
accuracy of one day, there follows that, first, the real time clock need not be

readable at a greater accuracy than that and, second, objects stored in the broadcast format can be freely used during that one day. If a stricter time control is to be applied, then more bits will have to be reserved in the frames and data groups for the time stamp.

5

For continuous operation of the real time clock the smart card has to be provided with a power supply, which is advantageously a small rechargeable battery that can be charged always when the smart card is connected to a receiver and/or playback device. When the battery voltage drops below a certain threshold value, the real
10 time clock is advantageously set in a shut-down state where its operation is prohibited, and it can be made operational again only by an authorized dealer at an authorized shop or through a secure two-way telecommunications link. The secret information needed for the removal of the shut-down state is advantageously stored in the permanent memory of the smart card when the card is delivered to the user. A
15 similar operation by an authorized dealer is required if the real time clock in the smart card has to be set to a new time, e.g. when crossing time zones, if the system does not use a certain standard time (such as the Greenwich Mean Time, GMT) in all its operations.

20 A device for an ordinary user which receives and/or reproduces digital objects can read and display to the user the time shown by the real time clock in the smart card but it cannot change it without authorization from an authorized dealer.

Referring to Figs. 1 to 4, it will be now described the selling and transferring of
25 various rights and corresponding keys in the system according to the invention enabling payments to the parties who own the rights related to the objects and/or their broadcasting. In the embodiments depicted by way of example the parties are the publisher (PUB; also content provider), broadcaster (BR; also service provider) and the user (U) of the object. The encircled numbers in the drawing represent one
30 possible mutual order of the various steps, without limiting the invention, though.

In the case depicted by Fig. 1, a user U buys from a representative of a publisher
PUB a record CD which contains the desired object. The publisher has manu-
factured the record in such a way that the data is in scrambled form (S) and the keys
35 needed for descrambling, which are included in the frames of the record (3j and 4j above), are encrypted. The price of the record corresponds to the manufacturing and transportation costs and does not include the charge for the right of use of the contents of the record. The key needed for decrypting the encrypted keys is called

an authorization and is marked A1. By paying the appropriate sum \$ the user gets the authorization.

The events in Fig. 1, in the order of their occurrence, are as follows:

5

① A publisher PUB produces a record CD in scrambled form (S) and attaches to it the encrypted keys. An authorization A1 is needed for decrypting the keys.

10 ② A user U pays to the publisher PUB both the price of the record CD and the charge \$ for the right of use of the contents of the record.

③ The publisher PUB gives to the user U the authorization A1 needed for the decrypting by storing it in the user's smart card SC.

15 ④ The user inserts the smart card SC and the record CD in a playback device (not shown) which then uses the authorization A1 to decrypt the keys and descrambles (US) the stored object while reproducing the object to the user.

20 The authorization A1 may be different and have different prices according to whether it entitles the user U only to use the stored object or also to copy it. The authorization may be publisher-specific, covering all products of a particular publisher, in which case the identification information related to the object in question has to be stored in the smart card SC in addition to the authorization. If the user later buys another product from the same publisher, the authorization need not be
25 loaded again in the smart card but only the identification information of the new product.

In the case depicted by Fig. 2, a user U acquires from a publisher PUB the right to use objects produced by said publisher and transmitted by a broadcaster BR. The
30 idea is that a publisher-specific authorization A1 and a certain amount of money are loaded in the user's smart card SC against a certain payment \$. The publisher PUB transfers an object to the broadcaster BR so that the object is already scrambled (S) and its scrambling keys are encrypted and require an authorization A1. The broadcaster broadcasts the object in question, which is then received and descrambled
35 (US) by a device of the user U using the authorization A1. The events in Fig. 2, in the order of their occurrence, are as follows:

① A user U pays to a publisher PUB a publisher-specific license fee \$.

② The publisher PUB gives an authorization A1 needed in the decrypting to the user U by storing it in the user's smart card SC. At the same time, a certain amount of "electronic money" \$\$\$ is loaded in the smart card.

5

③ The publisher transfers a scrambled (S) object to a broadcaster BR and attaches to it the encrypted keys. An authorization A1 is needed to decrypt the keys.

④ The broadcaster BR broadcasts the object.

10

⑤ The user inserts the smart card SC in a receiver and playback device (not shown) which then uses the authorization A1 to decrypt the keys and descrambles (US) the received object while reproducing the object to the user. At the same time, certain amount of electronic money in the smart card SC is marked spent.

15

Electronic money loaded in the smart card is marked spent in proportion as the user receives and uses broadcast objects. The amount marked spent advantageously depends on whether the user just reproduces the received object or stores it for later use. The identification information needed for identifying a certain object and the prices corresponding to the different purposes of use are broadcasted along with the object.

20

Fig 3. depicts a situation where a broadcaster BR purchases objects from a publisher PUB and distributes them free of charge to users U. The situation is otherwise the same as in Fig. 2, but the payments are made between the publisher PUB and the broadcaster BR, and the broadcaster BR gets the authorization A1 needed for the decryption. The broadcaster descrambles (US) the object and broadcasts it either entirely unscrambled or scrambled with unencrypted keys which the receiving device can read direct from the broadcast (cf. 3e and 4e above). Then, no money is marked spent in the user's smart card and, indeed, the user has no need for any authorization for which he should pay.

25

30

The concept of electronic money in connection with smart cards is known as such. A smart card may contain either "common money", meaning that an amount of money loaded in the smart card can be used for paying any charges to anyone, or money marked for a certain purpose. In the system according to the invention this means especially that common money could be used for paying for objects from any publisher, whereas money marked for a certain purpose, ie. for a single publisher.

35

could only be used for paying for objects coming from that particular publisher. The latter arrangement is the better since the publisher gets the money already in connection with the loading of the authorization, and there will be no confusion about what has been paid, to whom and for what services.

5

The embodiment of the invention described above, referring to Fig. 2, has the disadvantage that if a user has not acquired a publisher-specific authorization A1, he cannot use any objects from that particular publisher PUB broadcasted scrambled by a broadcaster BR. This disadvantage can be eliminated by an alternative embodiment according to Fig. 4 wherein a user U pays \$ for a broadcaster-specific authorization A2 and loads in his smart card electronic money marked for that broadcaster BR. A publisher PUB transfers an object to the broadcaster BR so that the object is scrambled (S) and its scrambling keys are encrypted and require an authorization A1. The broadcaster BR decrypts the keys and descrambles (US) the object but then
10
15
scrambles (S) the object again so that the new scrambling keys are encrypted and require an authorization A2. The broadcaster broadcasts the object which is then received and descrambled (US) by a device of the user U using the authorization A2.

20 If the agreement between the broadcaster BR and the publisher PUB requires that the publisher get paid according to how much the users have used the publisher's objects, the user's smart card SC divides the broadcaster-specific amount of money into publisher accounts and charges the accounts according to the use (direct use, storing, copying) of the objects. Later the user takes his smart card to be read by the
25
broadcaster, publisher or an authorized dealer, where the accounts are read and the broadcaster then has to pay the corresponding sums to the publishers. The smart card can also be read at the user's home through a secure two-way communications link. To motivate the user to have his card read, the authorizations can be arranged so that the user cannot later use a stored object before the respective accounts in the
30
smart card have been settled.

The events of Fig. 4, in the order of their occurrence, are as follows:

35 ① A publisher PUB and a broadcaster BR agree on broadcasting and the publisher PUB gives to the broadcaster BR an authorization A1 needed for decryption.

② A user U pays to the broadcaster BR a broadcaster-specific license fee \$.

- ③ The broadcaster gives to the user U an authorization A2 needed for decryption by storing it in the user's smart card SC. At the same time, a certain amount of "electronic money" is loaded in the smart card.
- 5 ④ The publisher PUB delivers an object in a scrambled form (S) to the broadcaster and attaches to it the encrypted keys. An authorization A1 is needed to decrypt the keys.
- 10 ⑤ The broadcaster BR uses authorization A1 to decrypt the scrambling keys and descrambles (US) the received object but then scrambles (S) it again so that authorization A2 is needed for the decryption. The broadcaster then broadcasts the object.
- 15 ⑥ The user inserts the smart card SC in a receiver and playback device (not shown) which then uses authorization A2 to decrypt the scrambling keys and descrambles (US) the received object while reproducing the object to the user. At the same time, certain amount of electronic money in the smart card SC is marked spent.
- 20 ⑦ If required by the agreement between the publisher and the broadcaster, the user has his smart card SC read, and the broadcaster BR pays license fees to the publisher PUB on the basis of the data in the smart card.
- 25 All above-mentioned authorizations loaded in the user's smart card can be valid for a fixed period of time or until further notice. The real time clock in the smart card is useful in the implementation of the fixed-period feature because then the receiver and playback devices need not have a clock. It is also more difficult to tamper with a clock in the smart card than with a clock in a certain device.
- 30 If the reception and use of an object are recorded in the smart card, it can be so arranged that by presenting his smart card to an authorized dealer the user is able to show that he has already paid for the use of the object and can then have the original record for a small extra charge as in Fig. 1.
- 35 The invention requires no changes in known object broadcasting media since the scrambling of digital objects in broadcasting is known in the prior art. A terminal equipment according to the invention has to include means for receiving and descrambling a transmission scrambled using a known method and for decrypting the scrambling keys by means of an authorization stored on a memory medium. In

- addition, a storing terminal equipment has to include means for producing the storage format described above in the storing phase, and for reading it in the play-back phase. These means are advantageously realized as software processes executed by a microprocessor controlling the operation of the terminal equipment or
- 5 another programmable device operating under its control, such processes being routinely drawn up by those skilled in the art.

Claims

1. A method for protecting digital media objects against unauthorized use, said objects being electrically distributable to several receivers and storable on a memory medium for later use, wherein a scrambled broadcast format is defined for said
5 media objects, **characterized** in that also a scrambled storage format is defined for said media objects for said storage on a memory medium, which scrambled storage format is different from said scrambled broadcast format.
2. The method of claim 1, **characterized** in that in said scrambled storage format
10 a media object is divided into frames which have a predetermined structure and contain actual data to be stored and other information related to the storage.
3. The method of claim 2, **characterized** in that to distinguish from said
15 scrambled broadcast format said other information in the frames includes a piece of information saying that the format is a storage format.
4. The method of claim 2 or 3, **characterized** in that at least part of said other
20 information in the frames is protected by including in the storage format a data part the contents of which is determined on the basis of the information to be protected in a manner determined by a secret algorithm.
5. The method of any one of the preceding claims, **characterized** in that said
25 scrambled broadcast format and scrambled storage format include a time stamp which in the broadcast format refers to the time of broadcasting and in the storage format to the time of storing.
6. The method of claim 5, **characterized** in that it is also required that when a
30 media object is reproduced to a user, it is examined whether the object in question is in the broadcast format, and if it is, the time stamp included in the broadcast format is compared to the time of reproduction, so that a difference greater than a pre-determined maximum between the time stamp in the broadcast format and the time of the reproduction prevents the object from being reproduced.
7. The method of any one of the preceding claims, **characterized** in that the
35 entitlement to use and/or store a particular media object is delivered to the user in the form of a key stored on a portable memory medium.

8. The method of claims 6 and 7, **characterized** in that the time of reproduction is read from a clock included in said portable memory medium.
- 5 9. Terminal equipment for receiving, storing and reproducing to a user digital media objects, comprising means for descrambling a scrambled broadcast format, **characterized** in that it also comprises means for storing a received media object in a scrambled storage format which is different from said scrambled broadcast format.
- 10 10. The terminal equipment of claim 9, **characterized** in that it comprises means to decode a time stamp included in the broadcast format in connection with the reproduction of the media object and to compare said time stamp to the time of reproduction.
- 15 11. The terminal equipment of claim 10, **characterized** in that it comprises means to read the time of reproduction from a portable memory medium.

1/4

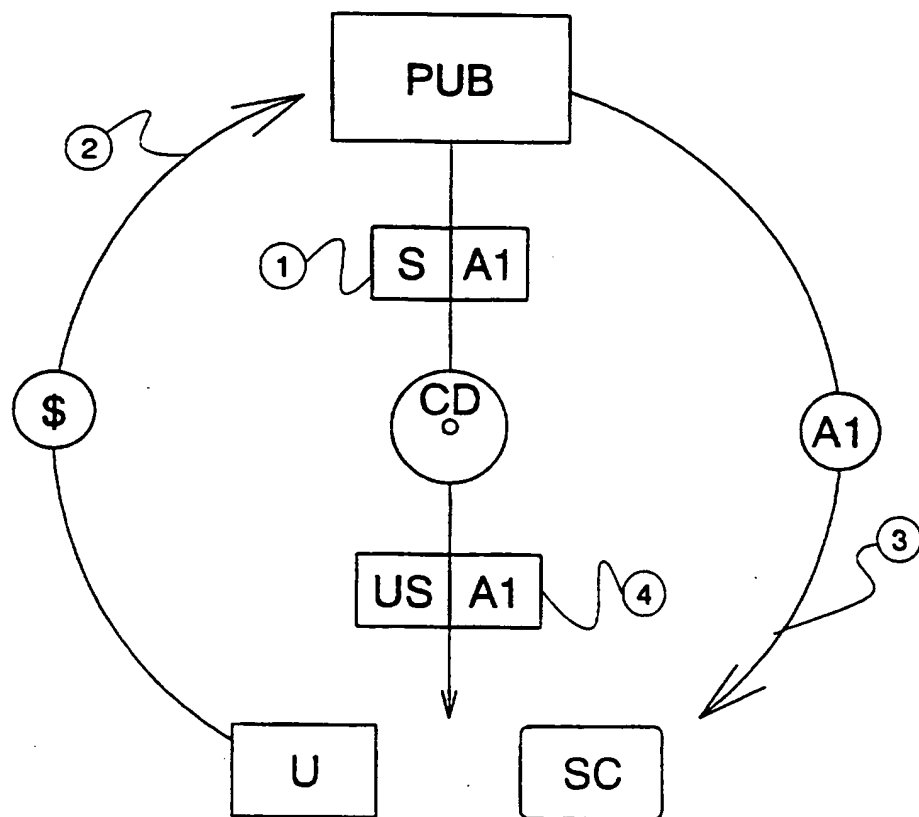


Fig. 1

2/4

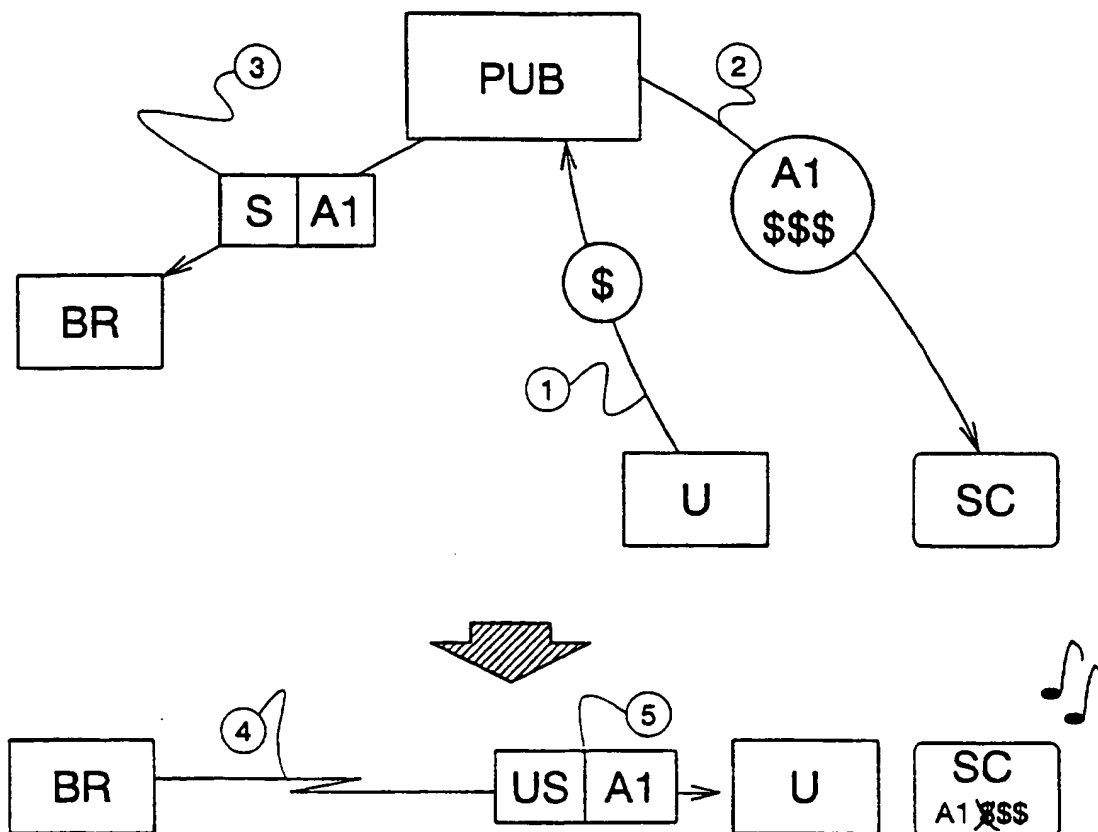


Fig. 2

3/4

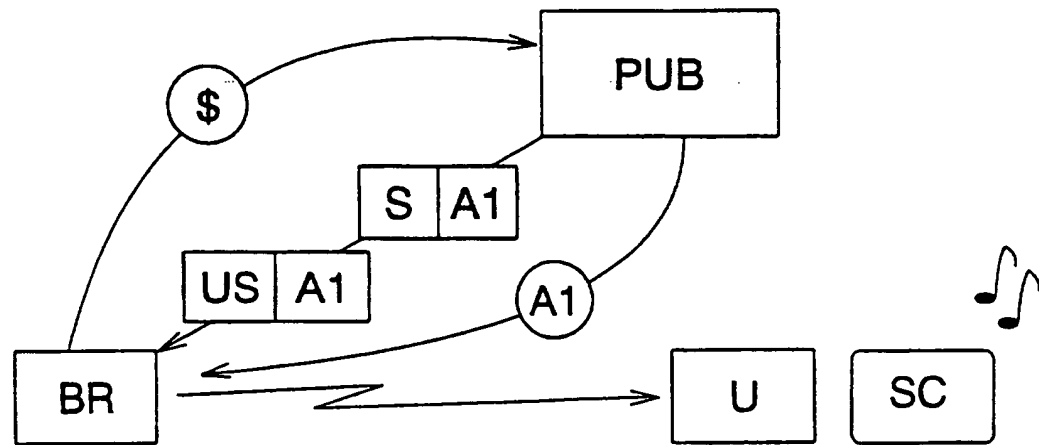


Fig. 3

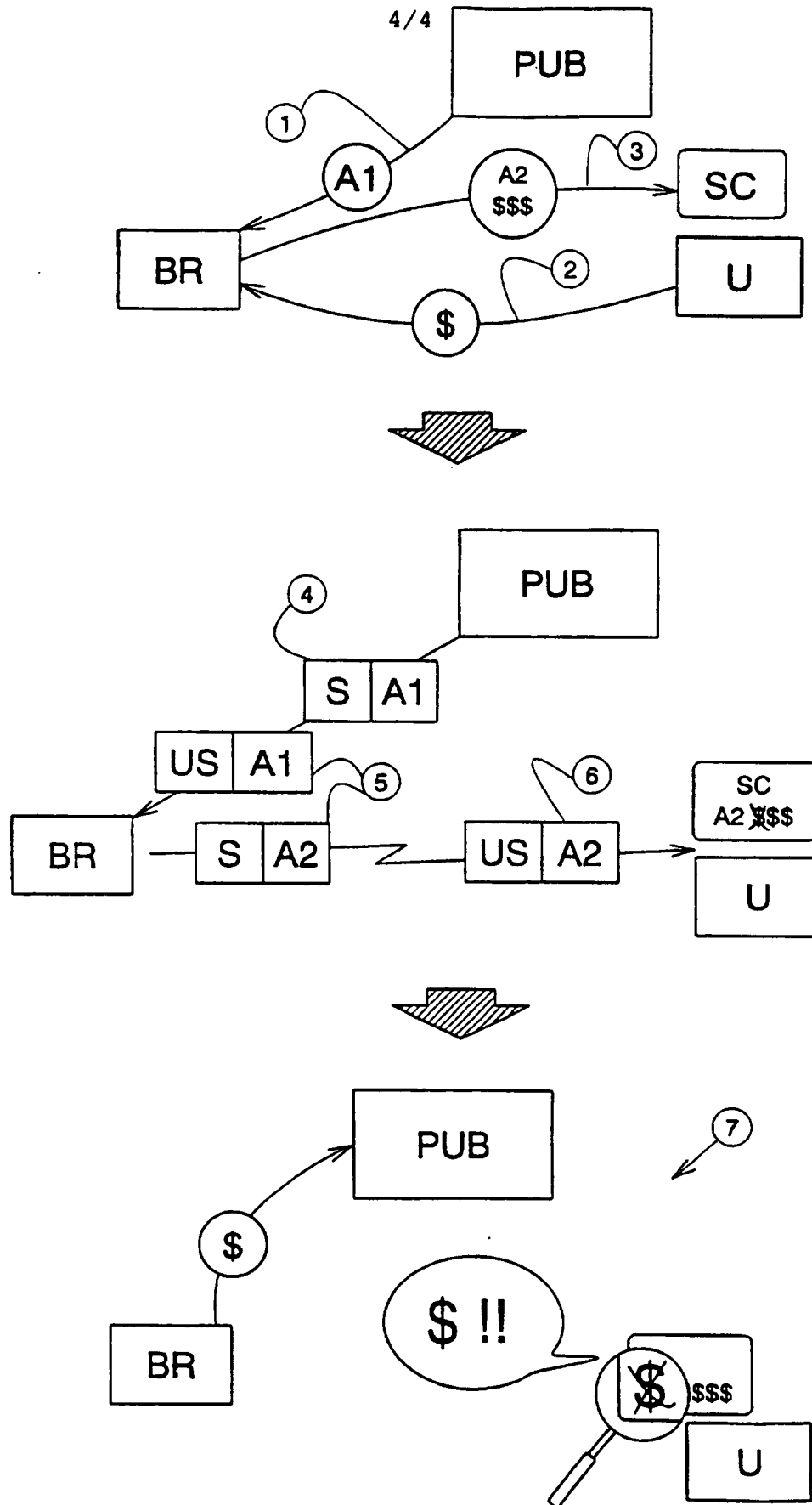


Fig. 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI 97/00045

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04N 7/167

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,A	EP 0710025 A1 (SONY CORPORATION), 1 May 1996 (01.05.96), abstract --	1-11
A	EP 0666694 A1 (GENERAL INSTRUMENT CORPORATION OF DELAWARE), 9 August 1995 (09.08.95), abstract --	1-11
A	WO 9113517 A1 (KUDELSKI S.A. FABRIQUE D'ENREGISTREURS NAGRA), 5 Sept 1991 (05.09.91), abstract --	1-11
A	EP 0674440 A2 (NOKIA TECHNOLOGY), 27 Sept 1995 (27.09.95), abstract --	1-11



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"B" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

29 April 1997

Date of mailing of the international search report

08 -05- 1997

Name and mailing address of the ISA/

Swedish Patent Office

Box 5055, S-102 42 STOCKHOLM

Facsimile No. +46 8 666 02 86

Authorized officer

Rune Bengtsson

Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT
Information on patent family members

02/04/97

International application No.
PCT/FI 97/00045

Patent document cited in search report			Publication date	Patent family member(s)		Publication date
EP	0710025	A1	01/05/96	JP	8181689 A	12/07/96
EP	0666694	A1	09/08/95	AU	676404 B	06/03/97
				AU	8150894 A	10/08/95
				CA	2137616 A	03/08/95
				JP	8107412 A	23/04/96
				NO	944678 A	03/08/95
				US	5504816 A	02/04/96
WO	9113517	A1	05/09/91	AT	147918 T	15/02/97
				AU	647080 B	17/03/94
				AU	7210691 A	18/09/91
				CA	2051810 A	22/08/91
				CH	682614 A	15/10/93
				DE	69124159 D	00/00/00
				EP	0469106 A,B	05/02/92
				HU	62131 A	29/03/93
				IL	97189 A	19/01/96
				JP	4505538 T	24/09/92
				US	5375168 A	20/12/94
EP	0674440	A2	27/09/95	FI	95756 B,C	30/11/95
				FI	941316 A	22/09/95

Form PCT/ISA/210 (patent family annex) (July 1992)

THIS PAGE BLANK (USPTO)